Submitted to Radiation Protection Dosimetry. Invited paper at the international seminar on Radiation Risk – Risk Perception and Social Constructions, October 19-20, 1995, Oslo

ON PROBABILISTIC RISK ANALYSIS OF TECHNOLOGICAL SYSTEMS

B. Natvig and J. Gåsemyr
Dept. of Mathematics, University of Oslo
P.O. Box 1053, Blindern, 0316 Oslo, Norway

Abstract – The reliability of a system is defined as the probability of system functioning. In reliability theory one is studying how the reliability of a system can be assessed from the reliabilities of its components. In the first part of this paper we consider the safety of a nuclear power plant from a reliability theory point of view. Especially one is focussing on the Chernobyl catastrophe in 1986 and the incidents at Le Bugey in 1984 and in Barsebäck 1992. Some main areas of modern reliability theory of interest for the safety of nuclear power plants are indicated. In the second part of the paper risk and risk aversion are considered by first showing how these concepts are applied in modern non-life insurance mathematics. At the end we discuss the link to the choice between different energy supplies.

RELIABILITY

The reliability of a system is defined as the probability of system functioning. In reliability theory one is studying how the reliability of a system can be assessed from the reliabilities of its components. At the 18th European Meeting of Statisticians in Berlin, GDR, on 22-26 August 1988, the first author organized a session on "Reliability of large technological systems". This topic was obviously a hot one at the time, due to e.g. the Chernobyl catastrophe on 26 April 1986. Some have claimed that this accident was totally unexpected; but this is to ignore the fact that even before the Three Mile Island accident on 28 March 1979, the American Reactor Safety Study[1] had been strongly criticized[2–3]. Laaksonen[4], of the Finnish Center for Radiation and Nuclear Safety, has expressed the following opinion on the Chernobyl accident:

> The Chernobyl accident provided a discouraging example of a phenomenon which would be extremely difficult, if not impossible, to foresee and take into account in a probabilistic risk analysis. Also the events which are usually considered in the safety analyses have almost been standardized 15 years ago.
>
> The accident took place when the operators were decreasing the reactor power, prior to taking the plant out of service for scheduled maintenance. A special test of electrical systems was to be made at the stage the reactor had reached the power of 700 - 1000 MW (20-30% of nominal power). At the beginning of the test the reactor was to be scrammed automatically and thus no interaction was expected between the reactor and the other plant systems.
>
> In the course of test preparation a coincidence of unfavourable operational steps brought the reactor to a state where it could reach prompt criticality in a few seconds.

The dangerous core characters were evoked by the operators who were lacking sufficient knowledge in reactor physics. During the 12 hours preceding the explosion the operators committed deliberately at least six severe violations of operating rules. Four of these were such that without any of them the accident would have been avoided:

1. Continued reactor operation without the necessary differential reactivity worth in the control rods (operation below the permissible value was indicated clearly on a computer printout).
2. Continued reactor operation below the minimum allowable power level.
3. Blocking of the reactor scram signals associated with steam drum level and reactor coolant pressure.
4. Blocking of the reactor scram signals associated with trip of both turbogenerator units.

The operator behaviour was of course unforgivable but I think it can be understood from the following viewpoints:

- a common attitude on operational rules in the Russian plants has been obviously quite relaxed: the rules have been taken as guidelines and not as strict orders
- the safety record of RBMK-reactors was good and no precursory events of this type had ever occurred
- Chernobyl unit 4 had an excellent reputation among the RBMK plants and the operators were evidently too selfconfident
- the operators were not able to raise the reactor power above 200 MW with the normal control systems (the power level followed changes in the coolant void content but the operators did not realize the situation clearly enough).

What the Chernobyl accident really did was to call into question the existing risk and safety analyses of large technological systems.

This was further underlined by the *Piper Alpha* oil-rig accident in the North Sea on 6 July 1988, where 167 people were killed. This issue will now be discussed more closely.

In applying reliability theory to such systems, the following problems arise:

- Lack of knowledge on the functioning of the system and its components;
- Lack of relevant data;
- Lack of knowledge on the reliability of the human components;
- Lack of knowledge on the quality of computer software;
- Lack of knowledge on dependencies between the components.

This makes it almost impossible to assess the probability of failure of a large technological system. Hence, the use of risk analysis to back political decisions on controversial safety issues is dubious, to say the least. If, however, a political decision has already been made, risk analysis and reliability theory can contribute essentially to *improving* the safety of a system. This is just the case for Norwegian offshore activities and for the Swedish nuclear power industry. It should, however, be noted that the latter is in some trouble after the incident in the Barsebäck 2 reactor on 28 July 1992. The site is very close to Copenhagen and the Danish environmental movement OOA has, also on the basis of a report[5] from

the first author, claimed the plant to be permanently closed down. Since Denmark has decided not to have nuclear power plants, the risk imposed by the nearby Swedish nuclear reactors is especially questionable from an ethical point of view.

The incident showed that the emergency core cooling system could fail rapidly, in case of a pipe rupture, due to a much faster than expected clogging of the strainer for emergency cooling water by washed down mineral wool insulation. The emergency core cooling system was modified and a socalled probabilistic safety analysis carried through during the autumn 1992. The Swedish Nuclear Power Inspectorate determined on January 4 1993 to restart the Barsebäck 2 reactor. The critique of this probabilistic safety analysis by the first author seems to be of general interest:

1. Just a very minor part of the documentation on the modified system was a proper probabilistic safety analysis and even this part was not very well founded. The rest was pure technical considerations.
2. No probabilistic safety analysis was done for the complete safety system of the reactor. Therefore, there was no sufficient guarantee that the introduction of the modified emergency core cooling system had not led to a weakening of the remaining safety system.
3. The sensitivity of wrong judgements in the safety analysis is tested by just varying one parameter at a time instead of a simultaneous sensitivity analysis of the parameters.

Undoubtedly, the analysis contributed to improve the safety of the system. However, as presented, it seemed to promise more. Hence the critique also concerns the communication and the information on the contents of the analysis. Generally, openness and honesty are key points in all sorts of communication, and of utmost importance when dealing with radiation risks due to public sceptisism.

To improve the safety of a system we need measures of the relative importance of each component for system reliability. Barlow and Proschan[6] suggested that the most important component is that having the highest probability of finally causing system failure by its own failure. The first author has since developed a theory supporting another measure[7]. The component whose failure contributes most to reducing the expected remaining lifetime of the system is the most important one.

The Chernobyl accident provided new data on nuclear power plants. What type of theory do we have to benefit from such data in future risk analyses in the nuclear industry? The characteristic feature of this type of theory is that one benefits both from data for the system's components and for the system itself. Furthermore, due to lack of sufficient data one is completely dependent on benefiting from the experience and judgement of engineers concerning the technological components and on those of psychologists and sociologists for the human components. This leads to subjectivistic probabilities.

The frequentistic interpretation of probability often makes little sense in dealing with risk analysis of rare events. However, both the subjectivistic and frequentistic probabilities are obeying the same natural rules of computation, based on the same axiomatic system, as

opposed to the corresponding concepts in fuzzy set theory.

The methodology of statistical inference that can deal naturally with subjectivistic probabilities[8] is called Bayesian after the English reverend and probabilist Thomas Bayes, who died in 1761. One starts out by using expert opinion and experience as to the reliability of the components. This information is then updated by using data on the component level from experiments and accidents. Based on the information on the component level, the corresponding uncertainty in system reliability is derived. This uncertainty is modified by using expert opinion and experience on the system level. Finally, this uncertainty is updated by using data on the system level from experiments and accidents.

Theory in this area is under development at the University of Oslo[9–10]. It should be noted that the use of expert opinions is actually implemented in the regulatory work for nuclear power plants in the US[11]. A general problem when using expert opinions is the selection of the experts. This problem is an important one needing further work. Asking experts technical questions on the component level[10], where the consequences for the overall reliability assessment on the system level are less clear, seems very advantageous. Too much experts' influence directly on system level assessments could then be prevented.

In the magazine *Nature*[12], there was an article on an incident coming close to a catastrophe, which occured in the night of 14 April 1984 in a French pressurized water reactor (PWR) at Le Bugey on the Rhône river, not far from Geneva.

> The event began with the failure of the rectifier supplying electricity to one of the two separate 48 V direct-current control circuits of the 900 MW reactor which was on full power at the time. Instantly, a battery pack switched in to maintain the 48 V supply and a warning light began to flash at the operators in the control room. Unfortunately, the operators ignored the light (if they had not, they could simply have switched in an auxiliary rectifier).
>
> What then happened was something which had been completely ignored in the engineering risk analysis for the PWR. The emergency battery now operating the control system began to run down. Instead of failing precipitously to zero, as assumed in the "all or nothing" risk analysis, the voltage in the control circuit steadily slipped down from its nominal 48 V to 30 V over a period of three hours. In response a number of circuit breakers began to trip out in an unpredictable fashion until finally the system, with the reactor still at full power, disconnected itself from the grid.
>
> The reactor was now at full power with no external energy being drawn from the system to cool it. An automatic "scram" system then correctly threw in the control rods, which absorbed neutrons and shut off the nuclear reaction. However a reactor in this condition is still producing a great deal of heat – 300 MW in this case. An emergency system is then supposed to switch in a diesel generator to provide emergency core cooling (otherwise the primary coolant would boil and vent within a few hours). But the first generator failed to switch on because of the loss of the first control circuit. Luckily the only back-up generator in the system then did switch in, averting a serious accident.

The article in *Nature* furthermore stated:

> But the Le Bugey incident shows that a whole new class of possible events had been ignored – those where electrical systems fail gradually. It shows that risk analysis must not only take into account a yes or no, working or not working, for each item in the reactor, but the possibility of working with a slightly degraded system.

In 1978 Barlow and Proschan initiated the development of a theory of reliability where both the components and the system are described in a more refined way than just as functioning or failing. During the 1980s, the University of Oslo has been central in the development of this theory[13]. It has also been indicated how this theory can be applied to offshore electrical power supply systems and pipeline networks. Furthermore, efficient algorithms and computer software based on this theory have been developed.

RISK AND RISK AVERSION

The risk notion is often used in an unprecise way not only in daily language, but also among socalled experts. The Norwegian Nuclear Power Commission Report[14] gives the following incorrect definition:

> "Risk is the probability of a certain undesirable consequence".

This contributes to a very unclear discussion of risk aversion in their work. The usual mathematical definition is[15]:

> "Risk is the expected loss of utility".

Hence risk is a weighted average of economical losses due to different consequences, with the corresponding probabilities as weights. The fruitfulness of this definition hopefully becomes evident from the following discussion of risk aversion.

An important contribution to modern non-life insurance mathematics is the application of utility theory in the treatment of the client's and the insurance company's risk assessments. Typical examples of problems that can be studied inside this theory are:

- Why is the insurance company willing to accept the risk which the client wishes to get rid of?
- What prize (premium) is the client willing to pay for insurance of a certain risk?
- How is a less likely major loss assessed compared to a more likely minor loss?

We consider a potential insurance client A, which will be referred to as a person, but might as well be a company, a society or another economical unit. A carries a risk that can cause him an economical loss in the coming year, such as a risk associated with fire and water damage or liability.

We assume that it is possible to give a simple number for the personal loss of utility A feels by loosing x dollars. Call this loss of utility $l(x)$. It may at first glance be considered reasonable to assume that the loss function is the straight line $l(x) = x$ shown in figure 1a. In this case A assesses a loss of 20 000 dollars to be twice as serious as a loss of 10 000

dollars. This may, however, not be true. It can be more reasonable to assume that the loss of the first 10 000 dollars is easier to accept than the additional last 10 000 dollars. If A in advance has lost a considerable part of his fortune, an additional loss of 10 000 dollars can cause serious personal consequences as executor's sale and loss of credit, leading to a significantly reduced standard of living and loss of social position and prestige.

These points of view indicate that the loss function should increase faster, the larger the loss is, as shown in figure 1b. A marginal loss of 10 000 dollars is then assessed as more serious, the larger loss A has suffered in advance.

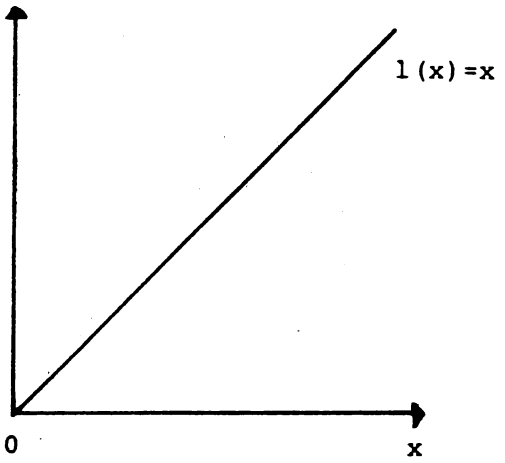

Figure 1a. A straight loss function

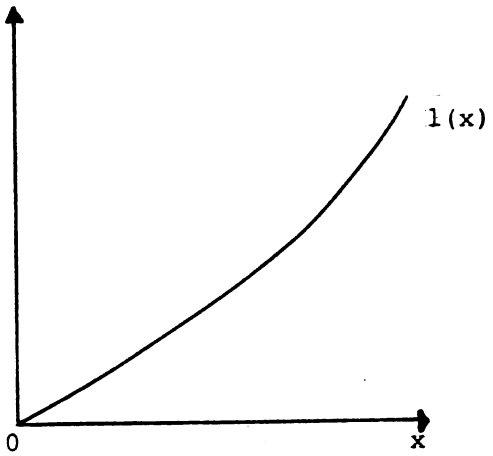

Figure 1b. A convex loss function

It can be shown that if A seeks insurance in spite of the fact that the premium is higher than the expected loss, then his assessment of loss is represented by the convex loss function of figure 1b and not the straight loss function of figure 1a. He is risk aversive making him prefer a fixed premium compared to a rather unlikely major loss, although the premium is larger than the average loss associated with the risk.

In insurance companies the premiums are considerably higher than the expected claims because the premiums, in addition to cover claims expenses, shall cover administration costs. Even so, people insure cars, houses and furniture and companies have fire, stock damage and product liability insurance. The clients' actual behaviour accordingly corresponds to the assumption of a convex loss function and we can conclude that they are risk aversive.

Now assume that A can choose between two risks R and S where R has the lowest damage probability whereas S has correspondingly smaller claims expenses if damage incurs, such that the expected annual claims expenses are identical for the two risks. It can then in a similar way be shown that A prefers the risk S compared to R. Due to risk aversion frequent, minor losses are preferred compared to rare major losses.

There are obvious similarities between A's choice of risk R or S and the society's choice

of nuclear, hydroelectrical or fossil power. If we without restrictions transfer the results above to the choice of different energy supplies, they can be formulated as:

- Two energy supply alternatives giving the same expected annual loss do not have to be assessed as equally risky. An alternative giving more frequent incidents with moderate consequences is, under otherwise equal conditions, preferred compared to an alternative giving more rare incidents with catastrophic consequences.

Especially, it follows that the risk associated with nuclear power is underestimated if one is only considering expected annual loss. The risk aversion is linked to the possible catastrophic nuclear power accidents.

The probabilities of different types and degrees of damage associated with energy production are not known exactly. The probability of construction site accidents may be satisfactorily estimated from statistical data, whereas the probability of serious accidents with a new nuclear reactor type must be estimated from reliability studies including limited data from other not completely similar reactors. The possibility of incorrectly estimating the damage probabilities enters as an extraordinary contribution to the risk, which from a risk aversion point of view disfavours the energy supply alternatives with the less certain estimated damage probabilities.

Generally, we hope that the readers have the risk aversion point of view in mind when discussing different sorts of radiation risk. It is not irrational to be risk aversive when confronted with great uncertainties.

ACKNOWLEDGEMENT

The section on risk and risk aversion is a shortened version of a section in a book[16] by the first author. The latter section was originally written by Professor Ragnar Norberg in 1979.

REFERENCES

1. Reactor Safety Study. *An Assessment of Accident Risks in US Commerical Nuclear Power Plants.* WASH-1400, Nuclear Regulatory Commission (Washington DC). (1975).

2. Lewis, H.W. et al. *Risk Assessment Review Group Report to the US Nuclear Regulatory Commission.* Nuclear Regulatory Commission (Washington DC). (1978).

3. Natvig, B. *Litt om Bruk og Manglende Bruk av Pålitelighetsteori i Kjernekraftutvalgets Innstilling (On the Use and Misuse of Reliability Theory in the Nuclear Power Commission Report).* The Faculty of Science, University of Oslo. (1979).

4. Laaksonen, J. *The Accident at the Chernobyl Nuclear Power Plant*, Society of Reliability Engineers, Scandinavian Chapter-Symposium, Otaniemi, Finland, 14-16 October 1986. Technical Research Centre of Finland, Electrical Engineering Laboratory, Otakaari 7B, SF-02150 Espoo, Finland. (1986).

5. Natvig, B. *Angående Probabilistisk Sikkerhetsanalyse (PSA) av Nødkjølningsfunk-*

sjonene ved Barsebäckreaktorene (On the Probabilistic Safety Analysis (PSA) of the Emergency Cooling Functions of the Barsebäck Reactors). Letter of May 6 1993 to the Director General of the Swedish Nuclear Power Inspectorate. (1993).

6. Barlow, R.E. and Proschan, F. *Importance of System Components and Fault Tree Events.* Stochastic Process. Appl. **3** (2), 153-173 (1975).

7. Natvig, B. *New Light on Measures of Importance of System Components.* Scand. J. Statist. **12** (1), 43-54 (1985).

8. Berger, J.O. *Statistical Decision Theory and Bayesian Analysis.* Springer Verlag (New York). ISBN 0 387 90471 9. (1985).

9. Natvig, B. and Eide, H. *Bayesian Estimation of System Reliability.* Scand. J. Stat. **14** (4), 319-327 (1987).

10. Gåsemyr, J. and Natvig, B. *Using Expert Opinions in Bayesian Prediction of Component Lifetimes in a Shock Model.* Math. Oper. Res. **20** (1), 227-242 (1995).

11. Chhibber, S., Apostolakis, G.E. and Okrent, D. *On the Use of Expert Judgements to Estimate the Pressure Increment in the Sequoyah Containment at Vessel Breach.* Nuclear Techn. **105** (1), 87-103 (1994).

12. Nature. *Near-Catastrophe at LeBugey.* **321**, 29 May, 462 (1986).

13. Natvig, B. *Multistate Coherent Systems.* In Johnson, N.L. and Kotz, S., eds. Encyclopedia Statist. Sci. **5**, 732-735. Wiley (New York). ISBN 0 471 05552 2. (1985).

14. Norwegian Nuclear Power Commission Report (NOU 35A). *Kjernekraft og Sikkerhet (Nuclear Energy and Safety).* The Oil and Energy Department (Oslo). ISBN 82 00 70449 1. (1978).

15. DeGroot, M. *Optimal Statistical Decisions.* McGraw-Hill (New York). (1970).

16. Natvig, B. *Sannsynlighetsvurderinger i Atomalderen (Probability Assessments in the Nuclear Age).* Universitetsforlaget (Oslo). ISBN 82 00 03325 2. (1987).